CYBER PHISHING - A THREAT FOR E-COMMERCEAND CONSUMER PROTECTION IN E-COMMERCE

Rajeshwari Suryakanth Nagamarpalli Alliance University
Bangalore, India
E-mail : rajeshwarinagamarpalli@gmail.com

ABSTRACT

The prevalence of smoothness of technology innovation has seen to have a skyrocket of cyberattacks. Ensuring the protection of personal information is significant about various data privacy laws. Emerging market trends have led to an increase in this field where everything from food to clothes to entertainment is being preferred online. So, this leads to the sharing of one's information online and hence paves way for such frauds.

Keywords: *Cyber-Crime; Cyber Phishing; Identity Theft; Financial Fraud; E-Commerce; Online Banking; Commercial Transactions; Consumer Protection; Emails; Cards; Deceptive Actions.*

INTRODUCTION

E-commerce has brought a big difference all over the entire world. On the contrary, theE-commerce sector in India has had spectacular growth over the past recent years but the E-commerce sector is still facingreal and serious challenges. The meaning of E- commerce is the buying and selling of goods and services through an electronic medium by the consumers. The OECD[1]states that E-commerce is a better approach for directing business, qualifying it as business happening overnetworks that uses non-proprietary conventions that are established through an openstandard-setting process, for example, the Internet.

The reason behind the increasingpopularity and acceptance of E- commerce all over the world is due to

1. The organization for Economic Cooperation and Development.

a great deal of convenience in commercial transactions with the support of the internet where the seller or merchant of the product can sell his products or offer his services directly to the consumer and the payment for the goods or services offered can be made electronically through various ways, for example, payment throughDebit or credit card or net banking. It is because of these conveniences and ease in doing business, the E-Commercemarket holds a great deal of value and has increased demand as well as it is expanding very fast and replacing most NonE-commerce transactions in varioussectors. E-commerce has already expanded in almost all areas of business and customer services[2].

With the rapid increase in usage of information and communication technology (ICT), various new branches of law have emerged, which are: Cyberlaw, Cyber Space Law or Information Technology law or Internetlaw to ensure law and order in cyberspace. A model law on E-commerce (MLEC) was adopted by the United Nations Commission on International Trade and Law (UNCITRAL) in 1996 and the mainfocus of the Model law on E-commerce(MLEC) was to bring forward a consistent law relating to E-commerce at a global level to bring Electronictransactions at a standard level with paper-based transactions discovering the rights and liabilities of the executing parties like those of paper-based transactions.

India enacted the Information Technology Act, 2000[3] as India was a signatory to the Model Law which wasadopted in 1996. Likewise, to give effect the UNCITRAL law on E- Signature (MLES), 2001[4] India enactedthe Information Technology (Amendment) Act, 2008[5].

It is just the beginning of the E- Commerce revolution in India and will envelop a lot more extensive scope of goods and services on a pan India basis in over a few years from now. E-commerce is generating lakhs of entrepreneurs each year, and that number can add upto lakhs and lakhs annually with a period of a year or two.

• INFORMATION TECHNOLOGY ACT, 2000

Information Technology Act, 2000 wasthe first law to be enacted by the GOI on E-commerce and the purpose of enactment of the IT Act, 2000 was to put into practice the UNCITRAL Model

2. "The Future of E-Commerce in India: Challenges and opportunities" 1 (12) IJAR 646 (2015)by Rajendra Madhukar Sarode
3. INFORMATION TECHNOLOGY ACT, 2000; Law Dealing With Electronic CommerceAnd Cybercrime.
4. UNICTRAL, The Model Law On Electronic Signatures (2001)
5. INFORMATION TECHNOLOGY AMENDMENT ACT (2008), further development of

Law on E-commerce, 1996. It was thenembraced by the General Assembly of the United Nations on 30th January 1997recognizing the Model Law on Electronic Commerce for a good consideration by the Member States as a Model Law when they order or overhaul their laws, taking into accountthe requirement for consistency of the law relevant to options to paper based techniques for communication and capacity of information.[6]

The only focus of the IT Act was to furnish a legalrecognition to the transactions that were carried out bythe mode of E-data interchanges and through some other mode of electronic communication, which is also calledE- commerce. The IT Act, 2000 paves a smooth way for E-commerce and E- governance in India. The IT Act holds provisions for legal recognition of E- records and E-signatures, rules for attribution for the E-record, for mode and way of affirmation, for deciding time and spot of dispatch and receipt of electronic records. The Act additionally builds up a regulatory framework and sets down discipline systems for various cybercrimes and offences. Offences such as hacking, breach of confidentiality and privacyand fraud concerning digital signatures were made punishable under the Act. Furthermore, the act provides for civil liability i.e. for Cyber and criminal violations.

The IPC 1860, The Indian EvidenceAct, 1872, and Reserve Bank of India, Act 1934 were also amended to take over the issues related to E-Commerce and crimes related E-commerce[7].

• INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

To give effect to The UNCITRAL Model Law on E-signatures 2001, India enacted the IT (Amendment) Act, 2008.The act has many known changes including the introduction of the conceptof E signatures.

The act also gave specific powers to the state to control websites for protecting privacy and also to keep track of misuse leading to tax evasions.The IT Act also gave legal validation toE-signatures and E-records for the veryfirst time in India and also emphasized securing E-signatures and E-records. These kindsof significant changes were brought forward to decrease electronic frauds.[8]

CHALLENGES AND LEGAL ISSUES FACED IN E- COMMERCE LAW

It is very normal to see disputes between parties when it comes to

6. Supra Note, 7
7. “Law Relating to E-commerce: International and National Scenario with Special Reference to

commercial relations. Problems or disputes may arise based on the contractual terms and negotiations. Disputes can arise in and out of the contractual terms which may be contractual or non-contractual. Copyright issues and data protectionissues are some of the examples of these kinds of disputes. Disputes in the B2C[9] segment which may be small in monetary terms, still involve problems such as problems in trans-border litigation and choice of law which are not at all convenient for consumers. Some of the legal issue and challenges are discussed hereafter:

ISSUES REGARDING VALIDITY OF THE E-CONTRACTS

The Indian Contract Act, 1887 governsall the E-contracts which are entered online. The acceptance of the terms & conditions before any purchase made online automatically implies a contract between the merchant and theconsumer. These kinds of implied contracts are known as "Click-wrap"contracts. Click Wrap contacts meanthat any contract is created by clicking on the 'I accept' tab. Another form of the well recognized implied contract includes the 'Browse-Wrap' Contract which is automatically created by browsing a certain website[10].

As a result, all the provisions under theContract Act, 1887 would automatically apply to an E-Commerce Transaction. All the necessary conditions of a valid contract are to be fulfilled as provided under the Contract Act. The necessary conditions which are to be fulfilled to consider a contract valid include free consent of the parties involved, the intention to enter into a legal contract and the capacity of the parties. These conditions can easily be defeated in E- commerce contracts very easily. Theterms & conditions in a website have to be in adherence to the Indian Contract Act, 1887 regardless of the agreements such as 'Click-Wrap or Shrink-wrap' to enter into a contract recognized by the IT Act[11]. All these aspects mentioned above are effective only in case of a dispute. Some of the problems that arise out of the E- commerce contracts make a contractvoid which renders the contract not acceptable i.e. inadmissible as evidencein the court.

Moreover, the E-contracts may be held unreasonable in itself or giving no alternative of negotiation. Then the question that arises here is whether suchstandard form of contracts is to be considered unreasonable and whether it should be struck down by the court. Such contracts have been opposed by the U.S. courts and have been treated as unreasonable and have been struck down considering the facts and situations of the cases. There are nowell-developed laws in India for

8. Business to Consumer

10 "E-commerce Laws In India: Foreign Investment And Retail Trade" 2-3 by JayanthPattanshetti Associates.

11. "Evolution of E Commerce in India: Challenges Ahead (Part 2)" 3 by M.M.K. Sardana.

considering the issue of whether onlineagreements are immoral. On the other hand, there are some legal provisions under the Indian Contract Act which discuss unreasonable contracts like when the object of the contract is averse to public policy. Therefore, The IndianContract Act does not offer much direction towards these kinds of serious problems.

PROBLEMS OF JURISDICTION IN DISPUTES:

The main constituents of E-commerce are taking orders, managing delivery ofthe product or service and collect E- payments. When such issues come up in such E-transactions, the complicationcan be irreparable and should be handled practically. The settlement of disputes in the B2C segment can be quite challenging. The disputes arising in E-commerce are mainly resolved with the physical territory where one or boththe parties to the dispute are located.In these types of cases, different kinds of principles are applied when it comesto different national jurisdiction.

The courts have laid down the guidelines to determine the jurisdiction based on the level of interactivity and the commercial nature of the exchange of information that takes place in a distinct jurisdiction. The activities are categorized into three areas:

a) Completely interactive websiteswhere their consumers buy goods and services, swap details or filesor enter into agreements;

b) Completely passive websiteswhere facts and figures are available as information for consumers to view.

c) Websites with limited interaction.

In the case of completely interactivewebsites, the courts mostly takejurisdiction over the out of state entrepreneur except in cases where the entrepreneur has forbidden E- transactions in the state. In the case of completely passive websites, they are not likely to be subject to jurisdiction asthey operate from outside the state[12].

Section 3 of the Indian Penal Code,1896 states that any person who is liableunder any Indian law who is going to be tried under any crime committed outside India should be handled in accordance with the provisions of the Indian Penal Code for any crime committed outside India in the samemanner as if the crime has been committed inside India.

Therefore, when it comes to cases of E-commerce, there is no properregulation in India to resolve the issue of jurisdiction.

• ISSUES CONCERNING PRIVACY

While completing any E-commerce transaction, it is almost very difficult to complete the E-transaction without gathering any personal data of the consumer such as the information about the consumer's identity and their financial information. E-Commerce

platforms tend to collect a variety of indirect butvaluable information such asthe preference of the consumers andsearch patterns along with the collectionof primary data from the consumers.

The concept of violation of privacy is dealt with in a very restricted sense under the Information Technology Act.The Act provides that the privacy of a person is said to be violated when images or pictures of their intimate bodyareas are captured or recorded and published or shared with the permissionof the person where the person would have a sensible expectation of privacy. The prescribed punishment for such crimes is imprisonment of up to 3 yearsor a fine amounting up to INR 2 lakhs[13].

But under the Information Technology Act, a notification has been issued under Section 43A which states that the Act contains a framework for data protection in relation to personal and sensitive data. The identity of a person is regarded as personal data and the information relating to bank accounts, or data related to payment instrument details often come under sensitive personal information. Due to the notification, obligations were cast for data protection in regard to personal data and sensitive personal data on punishment as given under the IT Act besides making the person liable formonetary reparations. Thus it is asked of the E-commerce platforms to have reliable instruments and arrangements in place so that they can be the legally correct position.

The E-commerce platforms have to protect their systems both internally andexternally from any unauthorized intrusion[14].

• ISSUES RELATED TO INTELLECTUAL PROPERTY RIGHTS

One of the prime concerns for any company entering into the E-commerce business is Intellectual Property. The internet is a place with no limited accessand a very minimum regulation, so therefore the biggest challenge in the E-business is the protection of Intellectual Property Rights. India has well-established framework for the protection of Intellectual Property Rights in the physical world, but on the other, the effectiveness of these laws and regulations to protect the rights of E- commerce transactions is not that simple.

Another burning issue is the disputes for domain names on which the Indian Law falls silent. A company that starts their business in E-commerce transactions would have to register for their domain name. A domain name in a very basic sense is an address on the internet. In more scientific terms, domain name is an easily distinguishableand significant name to the Internet Protocol Resource. The Domain names generally fall under Trademark law. Two identical domain names can never be registered in the domain name registry but it is possible that it quite possible that similar domain names can be

recorded. There is no particular law in India on Domain names excluding the judicial pronouncements which state thatdomain names are subject to trademarkprotection and are extremely valuable[15].

MAJOR ATTACKS THAT OCCURRED AND RESPECTIVE GRAPHS SHOWING HOW THEYPREVAILED AND LEAD TO DATA BREACH

PAYPALATTACK:

- 2019 was a major year for PayPalfor all the bad purposes. PayPal phishing shot up exponentially in2019 after a drop in phishing URLs in Q4 2018, rising 167.8 per cent in Q1 and consistently outpacing its peers for a total of 61,226 phishing URLs found by Vade Secure in 2019.[16]
- Everything which happens to exist online comes with a flaw of suspicion from suspicious emailsto suspicious websites to suspicious SMS. There is nothingthat can be relied on aptly or something which you can trust.
- Phishing on PAYPAL mostly takes place on the weekend asthe customers are free then and tend to shop or use their cards more frequently out for dinner oronline ordering of food, etc, whichmakes it easier for the data breach.
- Now PAYPAL to ensure consumer satisfaction and safety provides for anti-fraud protection,end-to-end payment offerings.

MICROSOFT ATTACK:

- The corporate Office 365 user base of Microsoft makes it a greatmatch for phishing on weekdays when users are in the office and most engaged in email. However, PayPal users include millions of non-business customers who are using the PayPal app. The essence of the business of PayPalmeans that, unlike business userswho can completely neglect email,customers will pay attention to account updates on weekends.[17]
- Microsoft Protector for Office 365 also offers simulations to helpyou recognise and correct phishingthreats in your enterprise.[18]
- The fraudsters use techniques like social engineering and timely subject lines to attract victims to click the emails and register their

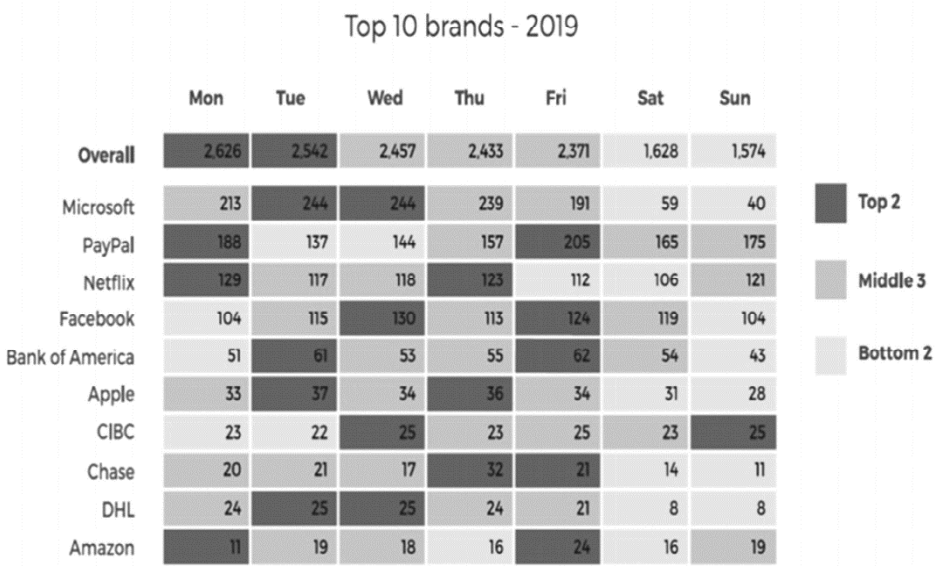
12. "E-Commerce Laws In The Indian Perspective, Sumanjeet
13. PayPal Phishing Hits an All-Time High by Adrien Gendre, 2019.
14. Zoom-Themed Phishing Campaign Targets Office 365 Credentials, https:// www.databreachtoday.com/zoom-themed-phishing-campaign-targets-office-365-credentials-a- 14600?
15. Terranova Security, pedagogical approach to cybersecurity, including gamification and interactive sessions designed to engage users' interests. The simulations are localized for

credentials, which are thencaptured.[19]

- On weekdays, Microsoft primarily faces crimes, as the office operates from Monday to Friday and then valuable details can be collected.

Nevertheless, the study also found that many of these teams lack adequate requirement structures that are a key component of the intelligence process and underpin proper intelligence output.

For policy-makers on cyber-security, thestudy offers authoritative guidance on:



AVERAGE OF PHISHING ATTACKS ON ORGANISATIONS ONWEEKENDS AND WEEKDAYS.[20]

2020 SANS CYBER THREAT REPORT[21] Shows Need for Better CTI Metrics

The number of organisations that fund full Cyber Threat Intelligence (CTI) programmes show tremendous growth in a recent study from the SANS Institute.

- Optimizing the combination of individuals, processes andresources to produce, ingest and act on information about threats.
- Comprehension and transcending inhibitors that hold back the CTI software.
- Identifying how to access the data

16. Phishing Campaigns Target Senior Executives via Office 365, https:// www.databreachtoday.com/phishing-campaigns-target-senior-executives-via-office-365-a- 14214?
17. Vade Secure for Cyber Security, March 26 2020.

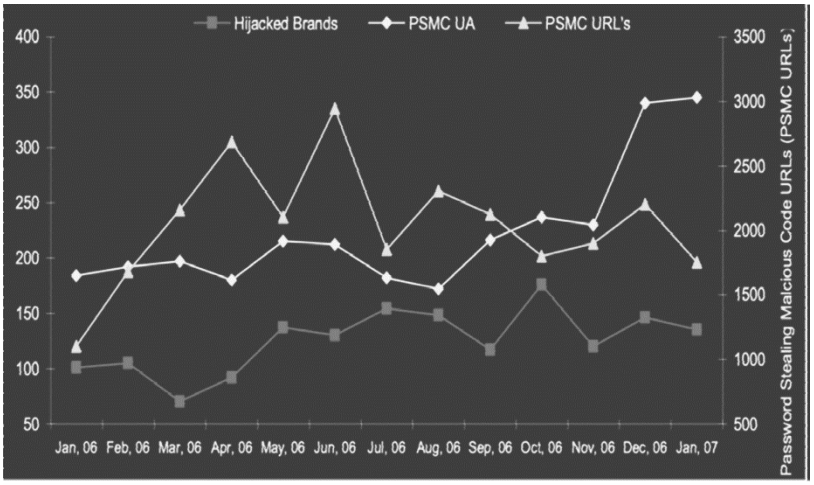
that will help respond to the most critical cyber threat

Furthermore, it can help save threat analysts considerable time by using automated tools to collect context on threat indicators for faster threat investigation.

Some phishing attacks have made a magnificent difference:

- In 2016, when hackers managed to get Hillary Clinton campaign chair John Podesta to cough up his Gmail address, maybe one of the most consequential phishing attacks in history occurred.
- The "fappening" attack, in which intimate images were made public to several celebrities, was originally assumed to be a result of vulnerability on the iCloud servers of Apple but was the outcome of a number of active data breaches.
- Employees at the University of Kansas replied to a phishing emailin 2016 and handed over access to their paycheck deposit records, causing them to lose pay.

From January 2006 to January 2007, the statistic shows the percentage of hijacked brands, the number of unique passwords which steal malicious code applications and the number of passwords which steal malicious URLs. While hijacked brands remained relatively stable throughout these months, numerous non-traditional websites were hijacked, such as social networking portals and gambling sites. As reported by APWG in the form of malicious code applications and URLs,the above diagram also shows several phishing-based Trojans. In the form of



HIJACKED BRANDS, PASSWORD STEALING MALICIOUS CODEAPPLICATIONS AND URLs[22]

malicious code applications and URLs that detect specific identity theft activity, as documented by APWG.

MALWARE DOWNLOAD (soft-targeted emails attack).

These kinds of phishing emails try to get the victim to infect their own machine with malware, like a lot ofspam. The messages are also "soft targeted"; for example, they may besent to an

HR employee with an attachment that purports to be the resume of a job seeker. These attachments are sometimes .zip files or malicious embedded code from Microsoft Office documents. Ransomware, the most common type of malicious code, is 93% of phishing emails are estimated to contain ransomware attachments.

In many distinct ways, phishing emails can be targeted. They are often not targeted at all as we noted; emails are sent to millions of possible victims totryto trick them into logging in to fake versions of very famous websites. The most famous brands hackers use in their phishing attempts have been countedby Iron Scales.

These were the top brand's attackers used from the 50,000-plus fake login pages the company monitored:

PayPal: Twenty-two per cent Microsoft:

Nineteen per cent

Facebook: Fifteen per centeBay: six

per cent Amazon: three per cent

Other times, attackers can send "soft targeted emails to someone who playsa specific role in an organisation, even though they don't personally know anything about them. Some phishingattacks are aimed at extracting logininformation from or infecting specific individuals' computers. Attackers devote even more resources to deceiving the victims, who were chosen because the possible rewards are very high.

CONSUMER PROTECTION IN E-COMMERCE

A report written by the Internet and Mobile Association of India disclosed that E-commerce market in India has almost reached USD 20 billion. Almost all the industries in India have been impacted by the E-commerce Industry,mainly the travel industry and online trading industry. The government of India has encouraged E-commerce platforms on a broad level which turns out to be a promotion of E-commerce activities.

Efforts have been madefor the protection of E-commerce as it is global as well as domestic in nature. The relationship between the consumers and the merchants who provide the good orservices is governed by the Consumer Protection Act, 1986[23]. It is noteworthy

---

that currently there is no specific act that regulates online transactions. The act has been carefully drafted to build up the confidence of the consumers in law and liability under the act arises only when there is a lack of services orin the case when the goods are defective in nature or in case of unfair trade practices. Any service that is freeof charge or cost is outside the scope of the Consumer Protection Act. Liability is triggered depending upon theactual seller who is selling off the goods.The distribution of goods comes under the Ambit of the act. Some of the various defences under the act are enlisted below:

- The defects in the goods will be removed.
- The goods will be replaced if defective.
- The amount spent on the purchased item will be returned in case of any discrepancy.
- Will discontinue any form of restrictive trade practices.

It is prohibited under the Consumer Protection Rules for E-commerce entities as well as merchants selling their products or offering their services from getting into any unfair trading practiceswhile conducting their business. The actin itself provides for an extensive explanation as to what constitutes unfairtrade practice. Following are the dutiesand liabilities under the act to address unfair trade practices:

Prohibition to fake false review and ratings:

Various market survey's conducted on e-commerce platforms have indicated that consumer reviews and ratings play a very important role when it comes to the customer's decision-making process. Fake reviews and ratings tend to distortthe views of the consumers which against the consumer's right to make an informed choice. Therefore the act prohibits any merchant or E-commerce based entity from falsely representing itself as a consumer and rating and reviewing their own products to gain customers.

- ***Authenticity of the product:***

The Consumer Protection Rules direct all E-commerce based entities and all the merchants selling their goods on alle-commerce platforms to make sure that their advertisements promoting their goods and services are uniform with the actual quality of the product.

- ***Prohibition on manipulating theprice of goods and services:***

The Consumer Protection Rules restrict any merchant or E-commerce based entities from procuring any unconscionable amount of profit by selling their product at a very high price.It is called engaging in the manipulationof prices of goods and services.

- ***Prohibition to discriminate:***

The Consumer Protection rules also state that no merchant or E-commerce based entities will discriminate betweentheir customers on the basis of sex, caste or creed. According to the rules, discrimination creates the arbitrary distinction between the customers which directly affects consumer rights.

DUTIES OF E-COMMERCE ENTITIES

a. All the E-commerce entities will have to provide the given necessary information to its consumers in a very clear and accessible manner:
   - Legal name of the entity
   - Address/location of itsheadquarters
   - Address/ Location of otherbranches
   - Name & details of theentity's website
   - Contact information of the entity such as email ID, phone number etc[24].

b. All E-commerce entities are prohibited from getting into any kind of unfair trade practices.

c. All the E-commerce entities are directed to set up a grievance redressal mechanism and appointa grievance officer.

d. All E-commerce entities will haveto make sure that the grievance officer takes up all the consumer complaints within 48 hours and redress it within a month.

e. If any of the E-commerce entities offer imported goods to its consumers, the entity has to mention the name and relevant information of the importer fromwhom the goods they're importing.

f. No E-commerce entity is allowedto charge a cancellation fee on their customers when the consumer has cancelled the goods after purchasing.

CONCLUSION

The fast and increasing growth of the E-commerce business has created a need for a functional regulatory framework that would ensure the success of the E-commerce industry in India. It has

always been pointed out that the cyber laws in India are not up to the mark and as there is no proper E-commerce regulatory framework available, there are so many challengesthat are being faced by the Indian consumers as well as the e-commerce industries in order to enjoy a consumer-friendly E-commerce environment.

Other than the Information TechnologyAct, India has no other regulatory framework which governs the E- commerce business in India. Therefore the Government should come up with a legal framework for E-commerce business in order for the business to grow successfully globally as well as nationally. For the E-commerce business to flourish, the basic rights of the consumers such as the right to privacy, prevention of fraud, intellectual propertyare to be taken care of. Also, it is an exclusive necessity for a specialized regulation to govern and regulate certainaspects of E-commerce business.

The Consumer Protection Rules a remarkable step towards better digital governance. But the execution of these rules would surge the operational costs of the E-commerce entities including small sellers. Therefore, the implementation of the rules will protectconsumers and their interests from unfair trade practices.

RECOMMENDATIONS

i. When it comes to consumerprotection, the areas defining return and exchange, informationrelating to the product and details about the seller should be specifically mentioned.

ii. As far as corporations and businesses are concerned they need to have software's which immediately detect cyber-attacks or when their information is beingtransferred to some other device or website.

iii. The current use of artificial intelligence can be used as one

of the efficient tools to detect identity theft and the deceptive actions of criminals where anotification can be sent to the user when such activity takes places.

iv. Cyber cells and authorities need to be more proactive inorder to combat this issue.

v. Stringent laws and punishments for these criminals must be givento deter them.

vi. 'Sandboxing' of emails can be helped to prevent suspicious/spamattacks.

REFERENCES

[1] Dalla, H. S., & Geeta. (2013).Cyber Crime – A Threat to Persons, Property,Government and Societies. International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), 997-1002.

[2] Desk, T. (2015, Aug 19). Ashley Madison hacked: Here's why the website for 'cheating spouses' got targeted. from http:// indianexpress.com/: http://indianexpress.com/article/technology/social/ashley-madison-data-breach-why-the-website-for- cheating-spouses-got-hacked/

[3] Dhanoa, R. (n.d.). Cyber Crime Awareness. International Journalin Multidisciplinary and AcademicResearch (SSIJMAR), 2(2), 1-7.

[4] Michael Totty (2002), "E- Commerce (A Special Report)",

[5] S. D. Vashistha (2005), "Ecommerce in Indian Perspective", The Business Review. March, 2005.

[6] Holz, Thurston (2005), "On the Economics of Botnets" available online at http://honeyblog.org/ archives/54-On-the- Economics- of-Botnets-Part-2.html

[7] Biever, Celeste, (2004), "How Zombie Networks Fuel Cybercrime" New Scientist, November available at http://www.newscientist.com/ article.ns?id= dn6616.

[8] Trend Micro, (2006), "Botnet threats and solutions", November, 2006 available online at http:// www.trendmicro.com.

[9] Microsoft, (2005), "Spear Phishing: Highly Targeted Scams", Microsoft, Corporation December,

2005.

[10] Lazarus, David, (2006). “Phishingexpedition at heart of AT&T hacking”, San Francisco Chronicle, September, 2006. availiable at www.sfgate.com.

[11] FCAC, (2006), “FCAC CautionsConsumers About New Vishing

[12] Schulman, Jay (2006). “Voice- over-IP Scams Set to Grow”, VoIP News, July, 2006.

[13] KrCERT/CC, (2006) “Korea Phishing Activity Trends Report”, Korean Internet Security Centre availableat http:// www.antiphishing.org/reports/ 200612 Korea Phishing Activity Report_Dec2006.pdf.

[14] Dan Ferguson (2006), “Phishing warning Beware e-mails asking for personal info, Peace Arch News”, Black Press, November, 2006, available at http:// www.peacearchnews.com/ portals-code/list.cgi?paper =44& cat=23&id=746625 &more=.

[15] Stevenson, Robert Louis B (2005), “Plugging the Phishing Hole: Legislation Versus Technology”, Duke Law and Technology Review 0006, 2005.

[16] Symantec Corporation, Internet Security Threat Report (2006), available at http:// www.symantec.com/specprog/ threatreport/ent-white paper_ symantec_internet_security_threat_ report_x_09_2006.en-us.pdf.